TESTIMONY OF
THOMAS N. PYKE, JR.
CHIEF INFORMATION OFFICER
U.S. DEPARTMENT OF ENERGY
BEFORE THE
SUBCOMMITTEE ON OVERSIGHT AND INVESTIGATIONS
COMMITTEE ON ENERGY AND COMMERCE
U.S. HOUSE OF REPRESENTATIVES

September 25, 2008

Good morning, Mr. Chairman. My name is Tom Pyke. I am the Chief Information Officer of the Department of Energy. The Office of the Chief Information Officer has responsibility for cyber security within the Department.

Over the last three years, the Department has undertaken a major effort to improve its cyber security posture. DOE has a comprehensive cyber security program that includes establishment of DOE-wide policy, a senior level governance structure, cyber security awareness and specialized cyber security training, improved cyber security incident management, and compliance monitoring.

The program is governed according to a Cyber Security Management Order that was issued in December 2006. This Order directs the use of a risk-based approach to cyber security management, and it establishes a governance structure within the Department that places primary responsibility for implementation of cyber security on the Under Secretaries, including the Under Secretary for Nuclear Security, who is the Administrator, National Nuclear Security Administration (NNSA), and other key leaders. These senior leaders determine and assess program-unique threats and risks, and they issue direction for implementing cyber security within their respective organizations.

In addition to the cyber security management order, we have issued a National Security Systems Manual, a Cyber Security Process Requirements Manual, and 18 cyber security "technical and management requirements" documents. This DOE-wide cyber

security direction builds on government-wide guidance from the Office of Management and Budget and Federal Information Processing Standards and other cyber security guidance issued by the National Institute of Standards and Technology, as well as applicable guidance issued by the Department of Defense. The Under Secretaries, the Administrator of the Energy Information Administration, the Power Marketing Administrations, and I have developed Program Cyber Security Plans that apply these DOE requirements as well as government-wide requirements within each of our DOE organizations.

Employing the risk-based approach, DOE senior management, including NNSA, has given special attention during the past year to the graded protection of DOE systems and data, taking into account threat and risk and the sensitivity of the data. As a part of this effort, it is appropriate for each part of the Department to review the sensitivity of the data under its jurisdiction relative to the strength of the controls that are in place to protect that data, and to strengthen those controls if needed after such a review.

The management of cyber security incidents is an integral part of cyber security management, including providing timely alerts to the entire Department of known threats, detecting cyber attacks as they occur or as soon as possible afterward, and responding to such attacks. The response includes reporting all cyber security incidents to the US-CERT, the Federal government's cyber incident handling center. It also includes mitigating the potential adverse impact of the incident, at the site at which it was detected and elsewhere in the DOE complex, determining the impact of the incident, and repairing any damage or disruption resulting from the incident.

DOE assists other agencies and receives information that helps DOE to defend its systems through participation in the interagency cyber security information sharing activities operated by the DOD Joint Task Force-Global Network Operations and other

organizations. We participate in the planning for and expect to benefit from planned activities of the government-wide Comprehensive National Cybersecurity Initiative.

Cyber attacks are increasing in complexity and frequency, and are becoming more aggressive. DOE is attacked over ten million times each day in a wide variety of ways, and DOE has defense-in-depth mechanisms in place throughout the complex. Even with this protection, some of the very sophisticated attacks on DOE have, on occasion, been able to penetrate our unclassified systems and networks. DOE has a cyber security defense based on industry and government best practices, and we continually improve our defenses, including our ability to detect attacks. However, some cyber attacks continue to evolve to avoid detection by these defenses.

Within the Department, the Office of the Chief Information Officer and NNSA cooperate in the reporting of cyber incidents and support to our sites as they handle cyber incidents. The Office of the CIO and NNSA have recently signed an agreement to improve further the way we work together to respond to cyber incidents. Our Office works in partnership with the Department's Office of Intelligence and Counterintelligence as we prepare for future cyber attacks and respond to them. Counterintelligence data analysis associated with activities that may have a foreign nexus provides useful input to the cyber security incident management process led by the Office of the CIO.

I would be pleased to respond to any questions you may have.